IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

SYNOPSYS, INC.,
                Plaintiff,

v.   Civil Action No. 3:21cv252

RISK BASED SECURITY, INC.,
                Defendant.

OPINION

The companies in this litigation—Synopsys, Inc. ("Synopsys") and Risk Based Security,

Inc. ("RBS")—identify and share with their customers software security vulnerabilities. After

Synopsys announced additional work it would perform in this area, RBS sent Synopsys a cease

and desist letter alleging that Synopsys's planned work would constitute copyright infringement

of RBS's database, misappropriation of RBS's trade secrets, and tortious interference with RBS's

current and prospective economic relationships. In response, Synopsys filed this suit seeking a

declaratory judgment that Synopsys's conduct does not so infringe, misappropriate, or interfere.

Each party has moved to exclude the other's experts and for summary judgment. After

reviewing the experts' reports and finding much material that will not aid the Court as the

fact-finder in this case, the Court will grant in part each party's motion to exclude. Because RBS's

experts' reports also suffer from reliability concerns, the Court will exclude the testimony of Ste-

ven Kursh in its entirety and will significantly limit the testimony of Adam Shostack.

The Court will deny each party's motion for summary judgment as to Count I, declaratory

judgment of no copyright infringement, because the parties dispute material facts regarding that

claim. For Count II, declaratory judgment of no trade secret misappropriation, the Court will grant

Synopsys's motion for summary judgment as to all of RBS's asserted trade secrets because RBS

has failed to establish that any of its materials satisfy the requirements for a trade secret. Lastly, for Count IV, declaratory judgment of no tortious interference, the Court will grant Synopsys's motion for summary judgment because RBS failed to establish the existence of any particular business expectancy.[1] The Court further explains these rulings below.

I. **FINDINGS OF FACT**[2]

A. Open Source Software and the Parties' Roles

"Open source software is software with source code available to anyone to inspect, modify, and enhance, and is widely used as the foundation for software applications across every industry." (ECF No. 227, at 11 ¶ 1.)[3] "Because it is so widely used, it is a target for hackers, as one open-source vulnerability can give hackers access to thousands of applications." (*Id.*)

Many initiatives have endeavored to identify and combat these vulnerabilities. The Open Security Foundation ("OSF") was a non-profit organization that ran the Open Source Vulnerability

---

[1] The Court previously dismissed Count III, a claim for copyright misuse. (ECF Nos. 128, 170.)

[2] The following facts include (1) those that the parties do not dispute, and (2) those that a moving party identified and the other party did not produce sufficient evidence to controvert. *See* Local Civil Rule 56(B) ("In determining a motion for summary judgment, the Court may assume that facts identified by the moving party in its listing of material facts are admitted, unless such a fact is controverted in the statement of genuine issues filed in opposition to the motion."); *see also Hodgin v. UTC Fire & Sec. Ams. Corp.*, 885 F.3d 243, 252 (4th Cir. 2018) (the nonmoving party "must produce evidence that goes beyond '[c]onclusory or speculative allegations' and rel[y] on more than 'a mere scintilla of evidence' to withstand summary judgment").
Because the parties filed cross-motions for summary judgment, the Court has "resolve[d] all factual disputes and any competing, rational inferences in the light most favorable" to the party opposing the relevant motion. *Rossignol v. Voorhaar*, 316 F.3d 516, 523 (4th Cir. 2003) (quoting *Wightman v. Springfield Terminal Ry. Co.*, 100 F.3d 228, 230 (1st Cir. 1996)); *cf. United States v. Carolina Transformer Co.*, 978 F.2d 832, 835 (4th Cir. 1992) ("On summary judgment, we must draw all justifiable inferences in favor of the nonmoving party, including questions of credibility and of the weight to be accorded particular evidence.").

[3] This Opinion cites to the page numbers assigned by the CM/ECF docketing system.

Database ("OSVDB"). (ECF No. 221-14, at 1.) OSVDB "provide[d] accurate and unbiased information about security vulnerabilities in computerized equipment." (*Id.*) In 2011, RBS acquired OSVDB from OSF in exchange for, among other things, "management resources, funding, and capital" support. (ECF No. 323-17, at 2; ECF No. 221-16.) RBS initially used the OSVDB data to create its own private software vulnerability database, VulnDB. Later, RBS used a subset of VulnDB data to update OSVDB. (ECF No. 227, at 13 ¶ 14 (citing ECF No. 234-6, at 231:21–232:6)); *id.* at 14 ¶ 15.)

The U.S. government also maintains a vulnerability identification initiative known as the Common Vulnerabilities and Exposures Program ("CVE Program").[4] (*Id.*) Through this program, a CVE Numbering Authority ("CNA") may "assign unique identifier numbers to vulnerabilities in open source security software and publish information about the vulnerabilities in the CVE Program's public catalogs." (*Id.* ¶ 3.) Synopsys became a CNA in March 2021. (*Id.* ¶ 2.) Since that time, Synopsys has disclosed certain vulnerabilities through the program. (*Id.* ¶ 3.)

RBS, formed in 2011, competes with Synopsys because RBS maintains a software vulnerability database, VulnDB. (*See id.* at 12–13 ¶¶ 5, 12.) Although competing in the market, RBS does not maintain total secrecy of its methods or products. CEO Jake Kouns has taught software users about the sources where vulnerability information "is . . . usually" or "should . . . be gathered." (*Id.* at 14 ¶ 18 (cleaned up).) Further, RBS provides demonstrations of the VulnDB portal to potential customers. Although RBS policy requires potential customers to first agree to certain confidentiality provisions, RBS has entered into licensing agreements with other businesses where the agreement did not explicitly require confidentiality for sublicensees. (*Id.* at 15 ¶¶ 21, 24–27;

---

[4] The Mitre Corporation runs this vulnerability identification program for the U.S. Department of Homeland Security. (*Id.* at 11 ¶ 2.)

ECF No. 341, at 13–14 ¶¶ 24–27.) RBS has also disclosed portions of its database schema on its

GitHub page.[5] (ECF No. 227, at 16 ¶ 28.)

B. Black Duck, its Programs, and its Files

Black Duck Software, Inc. ("Black Duck"), Synopsys's subsidiary, "offers its customers a

suite of analytical software and services to help customers manage their use of open source soft-

ware, and identify and track open source components in their software." (*Id.* at 11 ¶ 4.) In 2016,

Black Duck hired Chris Fearon as its Director of Security/Research. (*Id.* at 17 ¶ 32.) At that time,

Black Duck started to develop "the Threat Research Information Management System

('TRIMS')—a 'document management system' to allow Black Duck to interface with and store

vulnerability data." (*Id.*) Black Duck also developed Demeter, "a system of 'scrapers' that collect

vulnerability information" from mailing lists, RSS feeds, and other websites for TRIMS. (*Id.*

¶ 33.) Black Duck employees review vulnerability information in TRIMS and submit researched

vulnerabilities to the "Black Duck KnowledgeBase," where the vulnerabilities become available

to Black Duck customers as security advisories. (*Id.* ¶ 34.)

As a Black Duck employee, Fearon created several files that Black Duck used, at least in

part, to determine the public availability and accessibility of vulnerability references in the Vul-

nDB data feed,[6] (*see, e.g.*, ECF No. 228, at 15–16, 17 ¶¶ 1–4, 13; ECF No. 328, at 5–7, 10 ¶¶ 1–

4, 13; ECF No. 329-1, at 6–8), and one file the parties refer to as the "Python File," (ECF No. 228,

at 16 ¶ 6; ECF No. 328, at 7 ¶ 6). To complete the Python File, Fearon "needed to know the data

---

[5] RBS distinguishes its "database schema" from the "data structure" it claims as Copyright 58. (ECF No. 341, at 14–15 ¶ 28.)

[6] (*See generally* ECF No. 329-1 (describing the files Fearon created).)

4

structure of the VulnDB API."[7] (ECF No. 228, at 16 ¶ 7.) Once complete, Fearon used the Python

File to identify references appended to vulnerabilities in the VulnDB data feed. He then "de-

duplicated[8] the references to give the top level domains of each reference." (*Id.* ¶ 8.) The parties

no longer have access to many of these files, including the Python File. (ECF No. 329-1, at 4;

ECF No. 228-10, at 22:7–24:7, 27:15–29:13, 51:21–52:8.)

Another Black Duck file contains a "list of 920 VulnDB vulnerabilities that affect the top

1000 components listed on Black Duck's customers' bills of materials, which vulnerabilities are

not present in [the National Vulnerability Database ("NVD")]."[9] (ECF No. 328, at 11 ¶ 16; ECF

No. 228, at 17 ¶ 16.) Black Duck used this file "to understand the value of VulnDB to Black

Duck's customers." (ECF No. 228, at 17 ¶ 17; ECF No. 328, at 11 ¶ 17.) And yet another Black

Duck file "contains a list of vulnerabilities and references affecting the top 500 components listed

on Black Duck's customers' bills of materials, which vulnerabilities do not exist in NVD." (ECF

No. 328, at 12 ¶ 18; *see* ECF No. 228, at 17 ¶ 18.)

---

[7] The parties do not define "API" in their briefs. (*But see* ECF No. 341, at 20 (referring to API as "application programming interface").) The Court understands API to refer to "[c]ommands, functions, and protocols that allow software programs to communicate with specific operating systems or other software programs." Daniel B. Garrie, *Plugged In: Guidebook to Software and the Law Glossary*, Annotated Glossary, Westlaw (2022) (definition of "Application Program Interface (API)"); *cf. Phillips v. AWH Corp.*, 415 F.3d 1303, 1318 (Fed. Cir. 2005) ("Because dictionaries, and especially technical dictionaries, endeavor to collect the accepted meanings of terms used in various fields of science and technology, those resources have been properly recognized as among the many tools that can assist the court in determining the meaning of particular terminology to those of skill in the art of the invention.").

[8] De-deduplication means that Fearon recorded each reference only one time, even if a file mentioned it more than once. (ECF No. 228-10, at 249:18–21 (Fearon deposition).)

[9] "The NVD is the U.S. government repository of standards based vulnerability management data." NIST, *National Vulnerability Database*, https://nvd.nist.gov/ (last accessed Mar. 23, 2022).

Fearon also had access to a VulnDB data structure ("Data Structure 181790"), (ECF No. 228, at 18 ¶ 20; ECF No. 328, at 12 ¶ 20; *see also* ECF No. 329-2, at 157:4–12), which he analyzed to determine "the value being derived from the RBS feed for [Black Duck's] customers," (ECF No. 329-2, at 162:11–14; *see* ECF No. 228, at 18 ¶ 21; ECF No. 328, at 13 ¶ 21).

On December 11, 2017, Synopsys acquired Black Duck as a wholly owned subsidiary. (ECF No. 227, at 11–12 ¶ 4; ECF No. 228, at 18 ¶ 24; ECF No. 342 ¶ 10.) Before it did so, Synopsys conducted a due diligence review during which it "(1) evaluated [Black Duck Security Advisories ("BDSA")], (2) evaluated the BDSA source and reference list, and (3) had 'interaction with the technical people at Black Duck' who were involved in the development of BDSA." (ECF No. 228, at 18 ¶ 26.) "After Synopsys acquired Black Duck, the Black Duck employees who worked on BDSA/TRIMS became employees of Synopsys and Synopsys acquired BDSA." (*Id.* ¶ 25.)

C. The Reseller Agreement and the Massachusetts Lawsuit

On December 31, 2014, Black Duck and RBS entered into an End-User License Agreement ("Reseller Agreement" or "the agreement").[10] The agreement required Black Duck and Synopsys to maintain RBS's "Confidential Information," which the agreement defined as "non-public, technical and non-technical, written information whether in printed, textual, graphic or electronic form including but not limited to data, designs, specifications, processes, and all other business, product, and financial information." (ECF No. 221-11 § 10.1 (Reseller Agreement); *see also* ECF No. 228, at 18 ¶ 23; ECF No. 328, at 13 ¶ 23).) The Reseller Agreement also required that the parties "work

---

[10] The parties amended the agreement on November 13, 2017, and RBS later terminated it, effective December 31, 2018. (ECF No. 227, at 16 ¶ 31.) The amendment included a twelve-month "wind-down period." (ECF No. 221-34, at 2.)

together to integrate a feed from VulnDB into the [Black Duck Hub.]" (ECF No. 221-11, Ex. A § III; ECF No. 227, at 16 ¶ 29.) RBS did not give Black Duck or Synopsys permission to access any RBS source code. (ECF No. 227, at 16 ¶ 30; ECF No. 221-32, at 3–12.)

In 2018, RBS sued Black Duck in Massachusetts state court over issues relating to the Reseller Agreement. (ECF No. 227, at 17–18 ¶ 35.) On December 14, 2021, RBS added Synopsys as a party to that action. *RBS v. Black Duck*, No. 2084cv258-BLS2, Filing No. 129 (Mass. Sup. Ct. Dec. 14, 2021 (second amended complaint)).

The Massachusetts litigation has moved very slowly, with RBS apparently content to keep a cloud over Synopsys's head as long as possible. Seeking some resolution of the issues between the competing companies, Synopsys filed the instant case.

II. <u>DISCUSSION</u>

A. Motions to Exclude

Each party seeks to exclude the other's experts. Federal Rule of Evidence 702 permits expert testimony "in the form of an opinion or otherwise" by—

> [a] witness who is qualified as an expert by knowledge, skill, experience, training, or education . . . if:
>
> (a) the expert's scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue;
> (b) the testimony is based on sufficient facts or data;
> (c) the testimony is the product of reliable principles and methods; and
> (d) the expert has reliably applied the principles and methods to the facts of the case.

Fed. R. Evid. 702. A court may admit expert testimony under Rule 702 "if it concerns (1) scientific, technical, or other specialized knowledge that (2) will aid the jury or other trier of fact to understand or resolve a fact at issue." *Westberry v. Gislaved Gummi AB*, 178 F.3d 257, 260 (4th Cir. 1999).

7

In fulfilling its gatekeeping function, the Court must "ensure that scientific testimony is not only relevant, but reliable." *Kumho Tire Co. v. Carmichael*, 526 U.S. 137, 137 (1999); *see also Sardis v. Overhead Door Corp.*, 10 F.4th 268, 283 (4th Cir. 2021) ("To satisfy its gatekeeping duty under *Daubert*, the court must make an explicit reliability finding." (quoting *United States v. Ruvalcaba-Garcia*, 923 F.3d 1183, 1190 (9th Cir. 2019)). "Relevant evidence, of course, is evidence that helps 'the trier of fact to understand the evidence or to determine a fact in issue.'" *Nease v. Ford Motor Co.*, 848 F.3d 219, 229 (4th Cir. 2017) (quoting *Daubert v. Merrell Dow Pharm., Inc.*, 509 U.S. 579, 591 (1993)). "To be relevant under *Daubert*, the proposed expert testimony must have 'a valid scientific connection to the pertinent inquiry as a precondition to admissibility.'" *Id.* (quoting *Daubert*, 509 U.S. at 592).

"[T]he burden of establishing the reliability of the expert testimony is on the proponent . . . ." *Perkins v. United States*, 626 F. Supp. 2d 587, 592 (E.D. Va. 2009). In *Sardis*, the Fourth Circuit outlined the framework for a reliability analysis:

> Reliability is a "flexible" inquiry that focuses on "the principles and methodology" employed by the expert. *Daubert*, 509 U.S. at 594–95. Specifically, district courts must ensure that an expert's opinion is "based on scientific, technical, or other specialized *knowledge* and not on belief or speculation." *Oglesby v. Gen. Motors Corp.*, 190 F.3d 244, 250 (4th Cir. 1999). And to the extent an expert makes inferences based on the facts presented to him, the court must ensure that those inferences were "derived using scientific or other valid methods." *Id.*

> *Daubert* provides four, non-exhaustive "guideposts" to aid in the required reliability analysis: (1) whether the expert's theory or technique "can be (and has been) tested"; (2) "whether the theory or technique has been subjected to peer review and publication"; (3) "the known or potential rate of error" inherent in the expert's theory or technique; and (4) whether the expert's methodology is generally accepted in his field of expertise. *Nease*, 848 F.3d at 229 (quoting *Daubert*, 509 U.S. at 593–94). But this list "neither necessarily nor exclusively applies to all experts or in every case," as the relevance of some factors can "depend[ ] on the nature of the issue, the expert's particular expertise, and the subject of his testimony." *Kumho Tire*, 526 U.S. at 141, 150 (citation omitted). Accordingly, trial courts are typically given "broad latitude" to determine which of these factors (or some other unspecified factors) are "reasonable measures of reliability in a particular case." *Nease*,

> 848 F.3d at 229 (quoting *Kumho Tire*, 526 U.S. at 153). But that broad discretion does not allow a district court to delegate the issue to the jury.

Sardis, 10 F.4th at 281 (emphasis in original). "While a lack of testing is not dispositive," it remains an "especially important factor for guiding a court in its reliability determination." *Id.* at 290. "If the witness is relying solely or primarily on experience, then the witness must explain how that experience leads to the conclusion reached, why that experience is a sufficient basis for the opinion, and how that experience is reliably applied to the facts." Fed. R. Evid. 702 advisory committee's note.

"Rule 702 applies whether the trier of fact is a judge or a jury." *UGI Sunbury LLC v. A Permanent Easement for 1.7575 Acres*, 949 F.3d 825, 833 (3d Cir. 2020). But the standards relax when the judge sits as the trier of fact in a bench trial: "where the factfinder and the gatekeeper are the same, the court does not err in admitting evidence subject to the ability later to exclude it or disregard it if it turns out not to meet the standard of reliability established by Rule 702." *Larosa v. Pecora*, No. 1:07cv78, 2009 WL 3460101, at *3 (N.D.W. Va. Mar. 2, 2009) (quoting *In re Salem*, 465 F.3d 767, 777 (7th Cir. 2006)).[11]

Here, RBS seeks to introduce as expert witnesses Steven Kursh and Adam Shostack; Synopsys seeks to introduce Eric Cole. Having examined Kursh's, Shostack's, and Cole's extensive experience and other qualifications, the Court finds each expert qualified. But none of their testimony survives the Court's review unscathed, as each conveys improper legal conclusions,[12]

---

[11] The Court has "wide discretion" to determine "[w]hether an expert will assist the factfinder . . . 'particularly when the court sits as the trier of fact, for [it] is then in the best position to know whether expert testimony would help [it] understand the case.'" *Sun Yung Lee v. Clarendon*, 453 F. App'x 270, 278 (4th Cir. 2011) (quoting *Mercado v. Austin Police Dep't*, 754 F.2d 1266, 1269 (5th Cir. 1985)) (second and third alterations in original).

[12] (*See, e.g.*, ECF No. 212-5 ¶¶ 94, 96) (Cole report) (interpreting the parties' Reseller Agreement); ECF No. 212-6 ¶ 203 (Kursh report) (stating that Black Duck took actions "beyond

9

speculation,[13] or factual narrative.[14] Such material does not aid the Court as the fact-finder in this case.[15] The Court will exclude such material in each expert's report.

The Court finds many other faults in Kursh's report, which resembles a legal brief more than an expert opinion. Kursh reaches conclusions about Black Duck's actions, motives, and alleged trade secret theft based on inferences he draws from email exchanges, internal reports, and deposition testimony. In doing so, he inappropriately judges the credibility of witnesses and relies on adverse inferences the Court has not yet drawn.[16] (*See, e.g.*, ECF No. 212-6 ¶¶ 234–35, 460 (Kursh report).) Even more troubling is that Kursh willingly draws these conclusions despite admitting that he lacks information about the material he purports to evaluate.

---

the scope of allowed uses in both the original [Reseller] Agreement and the Amended Reseller Agreement").)

[13] (*See, e.g.*, ECF No. 212-1 ¶ 162 (Shostack report) (speculating that certain information "may be the time [the vulnerability] was imported"); ECF No. 212-6 ¶¶ 232, 346 (Kursh report) (generalizing based on one example and speculating as to the reason for a "massive spike in API calls").)

[14] (*See, e.g.*, ECF No. 212-1 ¶ 284 (Shostack report) (quoting a message from a Black Duck employee); ECF No. 212-5 ¶ 112 (Cole report) (quoting a former Black Duck employee's deposition); ECF No. 212-6 ¶¶ 299–301 (Kursh report) (quoting Black Duck emails and documents).)

[15] *United States v. Barile*, 286 F.3d 749, 760 (4th Cir. 2002) ("Expert testimony that merely states a legal conclusion is less likely to assist the jury in its determination."); *Oglesby*, 190 F.3d at 250 ("A reliable expert opinion must be based on scientific, technical, or other specialized *knowledge* and not on belief or speculation." (emphasis in original)); *City of Huntington v. AmerisourceBergen Drug Corp.*, No. CV 3:17-01362, 2021 WL 1320716, at *2 (S.D.W. Va. Apr. 8, 2021) ("Expert testimony which 'merely regurgitates factual information that is better presented directly to the jury rather than through the testimony of an expert witness' is properly excluded." (quoting *Hines v. Wyeth*, No. 2:04-0690, 2011 WL 2680842, at *5 (S.D.W. Va. July 8, 2011)).

[16] *See United States v. Dorsey*, 45 F.3d 809, 815 (4th Cir. 1995) ("[T]he evaluation of a witness's credibility is a determination usually within the jury's exclusive purview.").

For example, Kursh first outlines deficiencies in Black Duck's document production: "Black Duck provided several .csv files containing modest data, but none had metadata information to completely describe the extracted Black Duck information," (*id.* ¶ 173); "[t]here was also insufficient Black Duck evidence describing their Data Methods. One high-level Black Duck white paper-style document was provided to discuss data curation," (*id.* ¶ 177); "Black Duck provided no project plan documents," (*id.* ¶ 179); and "the Black Duck portal had minimal use in showing the Black Duck data," (*id.* ¶ 181).

Kursh then notes how the absence of these documents and data renders his analysis incomplete: "the metadata information is essential to accurately compare RBS data to the data in the Black Duck databases," (*id.* ¶ 173); "[w]ithout complete data extracts, I was forced to use what little data provided by Black Duck. With full extract of Black Duck data, I would be able to fully compare the RBS data to Black Duck," (*id.* ¶ 174); "I used the high-level information in th[e provided] document, but more details are necessary to get a fuller understanding of their methods," (*id.* ¶ 177); the lack of documentation "caused me to construct five project phased [sic] in a time-line format, using information from the other, albeit insufficient, Black Duck evidence," (*id.* ¶ 179); and the information in the Black Duck portal "is essential to fully understand Black Duck's usage of RBS data content trade secrets," (*id.* ¶ 181).[17]

---

[17] For some time, RBS sought Synopsys's assistance in "'stand[ing] up' [Black Duck's] files for meaningful analysis." (*See, e.g.*, ECF No. 187 (Special Master's recommendation for the parties to "arrange a brief meeting between their experts" for Synopsys's expert to "walk[] the RBS expert through the protocol he used to set up and evaluate the BDSA files").) Pursuant to the Special Master's recommendations on this issue, the Court established parameters for a meeting between the parties' experts. (ECF Nos. 240, 291.) In this Opinion, however, the Court bases its analysis on the information in the experts' provided reports, which include no meaningful analysis of Black Duck's products.

Kursh proceeds to disregard this catalog of deficiencies and to "compare" RBS and Black Duck documents.[18] Based on that comparison, he concludes that Black Duck used RBS's trade secrets. (*See, e.g.*, ECF No. 212-6 ¶ 406.) In other words, Kursh specifically states that he lacks the information necessary to perform complete analyses, but nevertheless provides opinions that far exceed the scope of permissible expert testimony. Based on this information, the Court cannot find Kursh's report reliable and must exclude it in its entirety.

Shostack's report suffers from many of the same flaws. For example, Shostack states that he could not "interact[]with [Black Duck's] databases in technical ways [to] allow [him] to understand their contents." (ECF No. 212-1 ¶ 19.) Later, in concluding that Black Duck copied data from VulnDB, Shostack evaluates a spreadsheet that was "produced [as] evidence in a document delivery that consisted of Black Duck documents." (*Id.* ¶ 221.) He was "provided no other context," but "assume[d] [the document] was from Black Duck." (*Id.* ¶ 222) Then, based on references to OSVDB in the spreadsheet, he concludes that the spreadsheet "is a copy of VulnDB which was not deleted at the end of the partnership." (*Id.*) This type of analysis—laden with speculation and lacking explanation of a reliable methodology—does not pass muster under Rule 702.

In addition, Shostack fails to demonstrate that he individually evaluated RBS's claimed trade secrets. Indeed, in his report he acknowledges that "another expert is examining the trade secrets individually," and that his report should "supplement, but not [] replace, any other RBS

---

[18] Black Duck did not produce a project plan, but Kursh still concludes that "there are five high-level Black Duck phases for the production of the TRIMS product," (ECF No. 212-6 ¶ 309); Black Duck did not provide "a dated export with explanations on the data content from the Black Duck databases," but Kursh nonetheless concludes that the "EXISTING" field in that document "shows Black Duck usage of the RBS VulnDB data" in a claimed trade secret, (*id.* ¶ 398); and Black Duck did not provide a "description of the data contained" in a particular Black Duck file, but Kursh still compares the values from that file to "a VulnDB export filename" based on an "assum[ption that] the file represents an export from an unnamed Black Duck database," (*id.* ¶ 384).

expert opinion." (*Id.* ¶ 215.) RBS argues that Shostack individually evaluated each trade secret and grouped them in his report only "to better educate the trier of fact." (ECF No. 339, at 5.) But the Court need not accept RBS's argument, and need not determine whether to permit this type of grouping, where Shostack admits that he did not individually evaluate each trade secret and RBS has not identified any evidence that shows otherwise.

Because Shostack did not understand the contents of Black Duck's products, the Court must exclude any of Shostack's testimony that purports to compare them to VulnDB or that opines on Black Duck's use of RBS's information. (*See, e.g.*, ECF 212-1 ¶ 31 ("Black Duck . . . made extensive use of [VulnDB] information to populate their products.").)[19] And, without an individual analysis of each claimed trade secret, the Court must exclude Shostack's conclusions about whether RBS's trade secrets satisfy any of the elements for trade secret misappropriation. (*See, e.g.*, ECF No 212-1 ¶¶ 28, 218 ("[T]he trade secrets contained within VulnDB . . . have independent economic value . . . .")); *see also MicroStrategy Inc. v. Bus. Objects, S.A.*, 331 F. Supp. 2d 396, 420 (E.D. Va. 2004) ("[T]he court must assess each alleged trade secret according to the requisite elements.").

The Court nonetheless finds that portions of Shostack's report discuss reliable principles and methods and remain relevant to the Court. He may thus testify about the concepts and industry standards applicable to this case, and may also provide background information on how individuals

---

[19] RBS argues that its experts did not need to compare VulnDB and BDSA because RBS can prove trade secret misappropriation through improper acquisition, rather than improper use, of its trade secrets. RBS correctly states the law, but does not direct the Court to any expert discussion of the improper acquisition of RBS's trade secrets. *See* Fed. R. Civ. P. 56(e); *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 257 (1986) (a party "must present affirmative evidence in order to defeat a properly supported motion for summary judgment").

in the industry analyze vulnerability data. Beyond these limited instances, the Court will exclude Shostack's testimony.

For Cole's report, the Court already explained above that it will exclude any legal conclusions, speculation, or factual narrative. The Court also understands that Cole based some of his opinions on a telephone conversation with former Black Duck employee Chris Fearon. As outlined below, the Court will exclude some and conditionally permit other portions of these opinions.

Federal Rule of Evidence 703 allows an expert to rely on otherwise inadmissible evidence "[i]f experts in the particular field would reasonably rely on those kinds of facts or data in forming an opinion on the subject." "[A]lthough an expert may rely on inadmissible materials in reaching his conclusion, Rule 703 'provides a presumption against disclosure to the jury of [inadmissible] information used as the basis for an expert's opinion . . . when that information is offered by the proponent of the expert.'" *Rambus, Inc. v. Infineon Techs. AG*, 222 F.R.D. 101, 111 (E.D. Va. 2004) (quoting 4 Jack B. Weinstein & Margaret A. Berger, *Weinstein's Federal Evidence* § 703.05 (2d ed. 2003)) (second alteration in original).

Here, if an expert in Cole's field would rely on a former employee's testimony in forming his opinions, then Cole may rely on Fearon's statements in doing so.[20] Cole may not, however, simply repeat any statements Fearon made during their conversation.[21] That type of parroting

---

[20] The Court may elicit additional information from Cole on this point at trial.

[21] (*See, e.g.*, ECF No. 212-5 ¶ 272 (Cole report) ("In fact, I asked Chris Fearon whether Black Duck ever used VulnDB as a source of vulnerability data, and in response, Chris Fearon explained to me that Black Duck never used VulnDB data as a source, and exclusively used publicly available sources, including public OSS lists, bugtraq, and others." (citing "Interview with Chris Fearon")).)

would not prove helpful where Synopsys may instead present Fearon's testimony directly to the Court.[22]

RBS's remaining concerns with Cole's testimony reflect disagreements with his methodologies or the factual bases of his opinions. These disagreements, on their own, do not render Cole's methodologies unreliable. As the fact-finder in this case, the Court will weigh the credibility of his remaining opinions at trial.[23]

B. Motions for Summary Judgment[24]

Under Federal Rule of Civil Procedure 56, a party may move for summary judgment on a claim, defense, or part of a claim or defense. The rule directs courts to grant summary judgment "if the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a). Because the standard asks whether

---

[22] Fed. R. Evid. 703 ("[I]f the facts or data would otherwise be inadmissible, the proponent of the opinion may disclose them to the jury only if their probative value in helping the jury evaluate the opinion substantially outweighs their prejudicial effect.").

[23] *Sun Yung Lee*, 453 F. App'x at 278; *see Verona v. U.S. Bancorp*, No. 7:09cv057, 2011 WL 13234383, at *2 (E.D.N.C. Aug. 23, 2011) ("Nothing requires that a rebuttal expert conduct the same analysis that the opposing expert did. . . . These subjects are proper for cross-examination but are not grounds to outright exclude the proposed . . . expert testimony."); *see also Fair Isaac Corp. v. Fed. Ins. Co.*, 447 F. Supp. 3d 857, 874 (D. Minn. 2020) ("[D]isagreements with the factual bases of [the expert's] opinions pertain to the weight and credibility of the opinions, not their admissibility.").

[24] Synopsys brings its claims under the Declaratory Judgment Act. Under the Act, the Court may "declare the rights and other legal relations of any interested party seeking such declaration, whether or not further relief is or could be sought." 28 U.S.C. § 2201(a). After the November 18, 2021 hearing, the Court held that RBS carries the burden of proof for Synopsys's declaratory judgment claims. (ECF No. 128); *see Medtronic, Inc. v. Mirowski Fam. Ventures, LLC*, 571 U.S. 191, 199–200 (2014) (finding that "the operation of the Declaratory Judgment Act [is] only procedural, leaving substantive rights unchanged" and that "the burden of proof is a substantive aspect of a claim" (internal citations omitted and cleaned up)). Any references to the "plaintiff's" burden herein thus refer to RBS.

any *genuine* disputes of material fact exist, the mere presence of some factual disputes does not defeat a properly supported motion for summary judgment. *Anderson*, 477 U.S. at 247–48. The party seeking summary judgment may succeed by establishing the absence of a genuine issue of material fact or showing that the other party cannot produce admissible evidence to support their claim: "a complete failure of proof concerning an essential element of the nonmoving party's case necessarily renders all other facts immaterial." *Celotex Corp. v. Catrett*, 477 U.S. 317, 323 (1986). When reviewing cross-motions for summary judgment, "the court examines each motion separately, employing the familiar standard under Rule 56 of the Federal Rules of Civil Procedure." *Desmond v. PNGI Charles Town Gaming, L.L.C.*, 630 F.3d 351, 354 (4th Cir. 2011).

a. Count I: Declaratory Judgment of No Copyright Infringement[25]

RBS "asserts Copyrights 51–58 and 60." (ECF No. 341, at 29; *see also* ECF No. 341-19, at 9–10 (Ex. V) (describing the asserted copyrights).) Synopsys moves for summary judgment because (1) "RBS has not adduced facts showing any infringement" for Copyrights 51–56; and (2) the Reseller Agreement permitted "Black Duck's use of any of alleged copyrighted material." (ECF No. 227, at 34.) RBS moves for summary judgment on (1) the second element for "Copyright 58 . . . [which] covers RBS's proprietary data structure for vulnerability information"; and (2) Synopsys's unclean hands defense. (ECF No. 228, at 33, 34.) The Court addresses each argument in turn.

---

[25] This Opinion addresses the parties' motions as of the March 1, 2022 hearing, when the case was still set for trial. After the Court denied the parties' motions for summary judgment as to Count I at the March 1 hearing, they filed a stipulation of dismissal without prejudice as to that count. (ECF No. 397.) Despite this dismissal, the Court will nevertheless explain its reasoning for denying summary judgment on this Count. (ECF No. 394, at 2 ("The Court will issue an opinion on these rulings."); *see also* ECF No. 398.)

1. Legal Standard

To prove copyright infringement, RBS must show that (1) it owns a valid copyright; and (2) Synopsys copied original elements of the copyrighted work.[26] *Humphreys & Partners Architects, L.P. v. Lessard Design, Inc.*, 790 F.3d 532, 537 (4th Cir. 2015), *as amended* (June 24, 2015). "An author gains 'exclusive rights' in her work immediately upon the work's creation, including rights of reproduction, distribution, and display." *Fourth Est.*, 139 S. Ct. at 887.

Although "originality is not a stringent standard," "the Constitution mandates some minimal degree of creativity." *Feist Publ'ns., Inc. v. Rural Tel. Serv. Co. Inc.*, 499 U.S. 340, 361 (1991). "[W]here a copyright is sought in a compilation, 'the principal focus should be on whether the selection, coordination, and arrangement are sufficiently original to merit protection.'" *Darden v. Peters*, 488 F.3d 277, 288 (4th Cir. 2007) (quoting *Feist*, 499 U.S. at 358).

---

[26] The Copyright Act also imposes a pre-suit registration requirement. Under 17 U.S.C. § 411(a), "no civil action for infringement of the copyright in any United States work shall be instituted until preregistration or registration of the copyright claim has been made in accordance with this title." *See also Fourth Est. Pub. Benefit Corp. v. Wall-Street.com, LLC*, 139 S. Ct. 881, 892 (2019) ("'[R]egistration . . . has been made' within the meaning of 17 U.S.C. § 411(a) not when an application for registration is filed, but when the [director of the Copyright Office of the Library of Congress] has registered a copyright after examining a properly filed application." (omission in original)). "[A]lthough an owner's rights exist apart from registration . . . registration is akin to an administrative exhaustion requirement that the owner must satisfy before suing to enforce ownership rights." *Id.* at 887; *see id.* at 888 ("In limited circumstances, copyright owners may file an infringement suit before undertaking registration. . . . Once 'preregistration . . . has been made,' the copyright claimant may institute a suit for infringement.").

RBS has not asserted that it has preregistered or registered any of the asserted copyrights, but it also has not filed any counterclaims in this suit. *Cf. supra* note 27. The Court may thus rule on RBS's rights "apart from registration." *See Fourth Est.*, 139 S. Ct. at 887.

2. Copyrights 51–56

In Copyrights 51–56, RBS cites to Black Duck files that no longer exist.[27] (*Id.* at 35; ECF No. 341, at 19, 34–35.) This is, of course, problematic for RBS, who has not produced evidence of the asserted copyrights in its own materials and bears the burden of proof on this claim. Despite this uphill battle, the Court finds summary judgment inappropriate because the parties genuinely dispute material facts regarding the files' contents.

Although the files no longer exist, RBS seeks to introduce evidence of their contents through the testimony of Fearon, the Black Duck employee who created them. (ECF No. 341, at 19–20.) Federal Rule of Evidence 1004(a) permits "other evidence of the content of a writing . . . if all the originals are lost or destroyed, and not by the proponent acting in bad faith." *See also In re Franklin*, 709 F. Supp. 109, 113 n.7 (E.D. Va. 1989) (collecting cases where courts admitted other evidence under Rule 1004). "[S]econdary evidence, presented pursuant to Fed. R. Evid. 1004, can be in *any* form." *In re Sol Bergman Est. Jewelers, Inc.*, 208 F.3d 215, 2000 WL 263338, at *4 (6th Cir. 2000) (Table) (emphasis in original). The fact-finder determines whether the "other evidence of content accurately reflects the content." Fed. R. Evid. 1008(c).

Neither party disputes that the original files no longer exist. Nor that RBS, the party seeking to admit other evidence of the files' contents, did not destroy them. RBS thus appropriately requests to introduce other evidence of the files' contents through the testimony of Chris Fearon. In his deposition testimony, Fearon confirms that one of the files "consists of data that [he] extracted from VulnDB." (ECF No. 341-12, at 245:6–8.) He also states that he created the files by "look[ing] at the references" for the vulnerabilities RBS distributed. (*Id.* at 248:14–249:7.)

---

[27] Black Duck destroyed the then-locally saved files RBS cites in these asserted copyrights when it "overwr[ote]" them in 2017. (ECF No. 227, at 20.)

Viewed in the light most favorable to RBS, RBS has "produced sufficiently clear evidence for a reasonable fact-finder to conclude that" the documents in question existed and the files included VulnDB content. *Klopman v. Zurich Am. Ins. Co. of Ill.*, 233 F. App'x 256, 260 (4th Cir. 2007). The Court will therefore deny this portion of Synopsys's motion for summary judgment.

3. Reseller Agreement

Synopsys says that the Reseller Agreement permitted Synopsys's alleged use of RBS's copyrights because the agreement authorized Black Duck to "use VulnDB data—without limitation—for its 'internal use.'"[28] (ECF No. 227, at 35.) The issue, then, is whether the agreement covered Synopsys's alleged use of this material.

"A licensee infringes the owner's copyright if its use exceeds the scope of its license." *Tattoo Art Inc. v. TAT Int'l LLC*, 498 F. App'x 341, 346 (4th Cir. 2012) (quoting *ITOFCA, Inc. v. MegaTrans Logistics, Inc.*, 322 F.3d 928, 940 (7th Cir. 2003)). "'[O]ne who obtains permission to use a copyrighted' work 'may not exceed the specific purpose for which permission was granted.'" *Id.* (quoting *Gilliam v. Am. Broad. Cos.*, 538 F.2d 14, 20 (2d Cir. 1976)).

---

[28] The Reseller Agreement labels Black Duck as the "Reseller" and, in turn, says the term Reseller includes Black Duck's "affiliates." (ECF No. 221-11, at 2.) The agreement then defines affiliate as "any corporation . . . that directly or indirectly owns, is owned by, or is under common ownership with [Black Duck] to the extent of at least fifty (50%) percent of the equity having the power to vote on or direct the affairs of the entity, and any person, firm, partnership, corporation, or other entity actually controlled by, controlling, or under common control with [Black Duck]." (*Id.*) Because Synopsys wholly owns Black Duck, and because neither party disputes that the agreement equally applies to Synopsys, for the purposes of this section the Court assumes without deciding that Synopsys must abide by and may benefit from the terms of the agreement.

In interpreting the terms and determining the scope of the Reseller Agreement in this case,[29] the Court must consider the contract as a whole[30] and interpret unambiguous language according to its plain meaning.[31]

> Contract language is ambiguous "only if it is susceptible of more than one meaning and reasonably intelligent persons would differ as to which meaning is the proper one." *Citation Ins. Co. v. Gomez*, 426 Mass. 379, 381, 688 N.E.2d 951 (1998). *See Fashion House, Inc. v. K Mart Corp.*, 892 F.2d 1076, 1083 (1st Cir. 1989) (ambiguity exists where terms are "inconsistent on their face or where the phraseology can support reasonable difference of opinion as to the meaning of the words employed and obligations undertaken"). However, "an ambiguity is not created simply because a controversy exists between parties, each favoring an interpretation contrary to the other." *Lumbermens Mut. Cas. Co. v. Offices Unlimited, Inc.*, 419 Mass. 462, 466, 645 N.E.2d 1165 (1995).

Id., 458 Mass. at 820–21, 941 N.E.2d at 640.

In the section of the Reseller Agreement that granted Black Duck a limited license, the agreement gave Black Duck a "non-exclusive, non-transferable, worldwide, license to," among other limited rights, reproduce VulnDB[32] into its products and sell access to VulnDB "only as incorporated into, or for use with, any [Black Duck] product" for a fee. (*Id.* §§ 2.2–2.2.2.) In the

---

[29] Because both parties cite contract interpretation principles under Massachusetts law in support of their arguments, the Court will similarly do so in interpretating the Reseller Agreement. (ECF No. 341, at 31; ECF No. 375, at 21.) The Court nevertheless notes that its conclusions would remain the same under Virginia law. *See Plunkett v. Plunkett*, 271 Va. 162, 167, 624 S.E.2d 39, 42 (2006) (outlining analogous rules of contract interpretation under Virginia law).

[30] *Wipro Ltd. v. Analog Devices, Inc.*, 527 F. Supp. 3d 93, 98 (D. Mass. 2021) (under Massachusetts law, "the contract must be considered 'as a whole' and '[i]ts meaning cannot be delineated by isolating words and interpreting them as though they stood alone'" (quoting *Farmers Ins. Exchange v. RNK, Inc.*, 632 F.3d 777, 785 (1st Cir. 2011)) (alteration in original)).

[31] *S. Union Co. v. Dep't of Pub. Utils.*, 458 Mass. 812, 820, 941 N.E.2d 633, 640 (2011).

[32] The agreement refers to the "Database," defined as RBS's "Basic VulnDB and the Premium Security Vulnerability," and including "all Intellectual Property embodied therein." (ECF No. 221-11 §§ 1.3, Ex A. § I.) The agreement defines "Intellectual Property," in turn, as including "copyrights." (*Id.* § 1.9.)

20

section on fees, the agreement provided that Synopsys would "not be required to pay a fee in connection with . . . [its] internal use (e.g. labs, testing, customer and product support related purposes)." (*Id.* at 5.)

Although the Court may interpret the parties' agreement as a matter of law, it must consider Black Duck's actions in determining whether Black Duck operated outside the scope of the agreement. *See Balles v. Babcock Power Inc.*, 476 Mass. 565, 571, 70 N.E.3d 905, 911 (2017). And, here, the parties dispute exactly what Black Duck's actions entail. Synopsys, for example, says that Fearon evaluated VulnDB for "customer and product support related purposes." (ECF No. 227, at 33.) RBS counters that Fearon conducted his VulnDB analysis for a competitive purpose: to "[r]eplace VulnDB with [a] proprietary solution." (ECF No. 341, at 32 (quoting ECF No. 341-12, at 53).) Because the parties dispute material facts regarding Black Duck's actions, the Court will deny this portion of Synopsys's motion for summary judgment.

4. Copyright 58[33]

RBS moves for summary judgment on "the second element [of copyright infringement]: that Synopsys copied original, constituent elements of Copyright 58." (ECF No. 228, at 33.) In support, RBS states that "[t]his data structure was original" and that Fearon "testified that he copied this structure from VulnDB in May 2016." (*Id.*)

For the second element of copyright infringement, RBS must show that Synopsys copied original elements of the copyrighted work. *Humphreys*, 790 F.3d at 537. Other than its bald assertion that Copyright 58 "represents an original arrangement and selection of facts about

---

[33] Copyright 58 is "[t]he arrangement and selection of data reflected in BD-RBS-181790-91" (the "Data Structure"). (ECF No. 228-28, at 2.) BD-RBS-181790-91 refers to the portion of Fearon's VulnDB analysis that contains a data structure. (*See* ECF No. 341-12, at 42–43.)

software vulnerabilities," (*id.* at 34), though, RBS cites no evidence and provides no explanation for what makes the arrangement original.

In its reply brief, RBS attempts to divorce the copying and originality requirements of the second copyright infringement element, arguing that the Court should grant summary judgment on "copying" alone.[34] But this element necessarily requires that RBS prove originality of at least portions of the copyrighted material. *See Humphreys*, 790 F.3d at 537 ("[A] plaintiff must prove that . . . the defendant copied the *original elements* of that copyright." (emphasis added)). Minimal as the originality requirement may be,[35] it certainly demands more than the unsupported assertions here.[36] The Court will deny this portion of RBS's motion for summary judgment.

5. Unclean Hands Defense

In an interrogatory response, Synopsys stated that "[a]ny copyright RBS might have in VulnDB is . . . [un]enforceable because of RBS's unclean hands."[37] (ECF No. 223-29, at 2.) RBS seeks to prevent Synopsys from asserting this defense at trial.

---

[34] A plaintiff who lacks direct evidence of copying "may prove copying by circumstantial evidence in the form of proof that the alleged infringer had access to the work and that the supposed copy is substantially similar to the author's original work." *Bouchat v. Balt. Ravens, Inc.*, 241 F.3d 350, 353 (4th Cir. 2001); (*see* ECF No. 328, at 12 (Synopsys admits that Fearon's analysis "depicts a data structure from VulnDB.").)

[35] "Original, as the term is used in copyright, means only that the work was independently created by the author (as opposed to copied from other works), and that it possesses at least some minimal degree of creativity." *Feist*, 499 U.S. at 345.

[36] RBS's bald assertions fail to establish that the data structure in Copyright 58 "was independently created by [RBS] (as opposed to copied from other works)"—including, for example, as opposed to being copied from another database like OSVDB. *Id.*

[37] Synopsys denies asserting an affirmative defense, noting that RBS has not filed any counterclaims in this action. But Synopsys nevertheless argues that it remains "entitled" to introduce evidence in support of this defense. (ECF No. 328, at 23 n.5.)
The Court previously ruled that RBS carries the burden of proof for the underlying claims in this declaratory judgment action, and since that time the parties have approached the action as

The doctrine of unclean hands prevents a plaintiff from seeking equitable relief if he is "tainted with inequitableness or bad faith relative to the matter in which he seeks relief, however improper may have been the behavior of the defendant." *Precision Instrument Mfg. Co. v. Auto. Maint. Mach. Co.*, 324 U.S. 806, 814 (1945); *see Food Lion, Inc. v. S.L. Nusbaum Ins. Agency, Inc.*, 202 F.3d 223, 228 (4th Cir. 2000) (Under Virginia law, the doctrine of "[u]nclean hands bars a party from receiving equitable relief because of that party's own inequitable conduct."). Such a defense does not apply here, where RBS seeks solely legal, rather than equitable, relief.[38] *See Food Lion, Inc.*, 202 F.3d at 229. The Court will grant this portion of RBS's motion.

b. Count II: Declaratory Judgment of No Trade Secret Misappropriation[39]

Synopsys moves for summary judgment on this Count because (1) RBS does not have any legally protectable trade secrets; and (2) RBS cannot prove that Synopsys misappropriated any of its trade secrets. RBS moves for summary judgment on twelve claimed trade secrets, stating that (1) Synopsys improperly used and acquired such trade secrets; and (2) Synopsys's independent development defense fails as a matter of law. The Court addresses Synopsys's and then RBS's motions in turn.

---

if RBS filed the suit. *See supra* note 27. Synopsys, in effect, has assumed the role of the defendant. By asserting unclean hands during discovery and maintaining its right to assert such a defense at trial, Synopsys has made this defense a potential issue, and the Court finds it proper address it at this time.

[38] "Equitable jurisdiction refers to the authority of the court to impose a remedy that is not available at law." 30A C.J.S. Equity § 1; *see also Tiller v. Owen*, 243 Va. 176, 179, 413 S.E.2d 51, 53 (1992) ("A trial court must have a cognizable basis for granting equitable relief.").

[39] Of the 160 trade secrets RBS disclosed, it now asserts that Synopsys misappropriated only the following: Trade Secrets 1–16, 19–23, 25–49, 52–62, 68, 77, 84, 86, 90–91, 94–96, 99–100, 105, 108, 110, 112–113, 115, and 118. (ECF No. 228, at 19 n.2; ECF No. 228-26.)

1. Legal Standard[40]

To prove trade secret misappropriation, a plaintiff must show "(1) the existence of a 'trade secret'; and (2) the 'misappropriation' of that trade secret by the defendant."[41] *Space Sys./Loral, LLC,* 306 F. Supp. 3d at 854 (quoting *Trident Prods.& Servs., LLC v. Canadian Soiless Wholesale, Ltd.,* 859 F. Supp. 2d 771, 778 (E.D. Va. 2012), *aff'd,* 505 F. App'x 242 (4th Cir. 2013)); *see* 18 U.S.C. § 1836(b)(1).

Under the VUTSA, "an alleged trade secret must 'meet all the criteria listed in the statute: (1) independent economic value; (2) not known or readily ascertainable by proper means; and (3) subject to reasonable efforts to maintain secrecy.'" *Space Sys./Loral, LLC,* 306 F. Supp. 3d at 855 (quoting *Trident Prods.,* 859 F. Supp. 2d at 778).[42]

---

[40] Synopsys brings its claims under the Defend Trade Secrets Act ("DTSA") and the Virginia Uniform Trade Secrets Act ("VUTSA"). RBS argues, however, that Massachusetts law must govern this claim because of a choice of law clause in RBS and Black Duck's Reseller Agreement. (ECF No. 228, at 19 n.3; *see* ECF No. 221-11 § 13.11) The parties did not brief this issue in their motions for summary judgment, and the Court has not yet determined whether the choice of law clause applies to the trade secret claims in this action. (*But see* ECF No. 170, at 7–11 (finding that RBS "waived its right to enforce" the agreement's forum-selection clause).) The Court will thus rely on the DTSA and VUTSA in its analysis. The Court notes, however, that substantially similar standards apply under federal, Virginia, or Massachusetts trade secret law, and that its conclusions remain the same under any of these regimes. *See OROS, Inc. v. Dajani,* No. 1:19cv351, 2019 WL 2361047, at *2 (E.D. Va. June 4, 2019) ("[I]n critical respects, the applicable standards under the DTSA and under state-law analogues—for instance, the VUTSA—are nearly identical."); *Moog, Inc. v. ClearMotion, Inc.,* No. 1:19cv12066, 2020 WL 6162921 (D. Mass. Oct. 21, 2020) ("The standards for misappropriation under the DTSA and the Massachusetts statute are substantially similar."); (*see also* ECF No. 228, at 19 ("Courts construe the federal, Virginia, and Massachusetts trade secret statutes in light of the Restatement (Third) of Unfair Competition.")).

[41] Under the DTSA, the plaintiff must also show that the trade secret "implicates interstate or foreign commerce." *Space Sys./Loral, LLC v. Orbital ATK, Inc.,* 306 F. Supp. 3d 845, 853 (E.D. Va. 2018).

[42] A trade secret must "[d]erive[] independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use." Va. Code § 59.1-336.

> [T]o prove misappropriation, the plaintiff must establish two elements: (1) that the defendant acquired, disclosed, or used a trade secret developed by the plaintiff through improper means (namely, without express or implied consent); and (2) that the defendant knew or had reason to know that its knowledge of the trade secret was either acquired under circumstances giving rise to a duty to maintain its secrecy or derived through a person owing such a duty to the plaintiff.

Id. (citing *Trident Prods.*, 859 F. Supp. 2d at 778).

The DTSA defines trade secrets as "all forms and types of financial, business, scientific, technical, economic, or engineering information" that "the owner thereof has taken reasonable measures to keep . . . secret." 18 U.S.C. § 1839(3). The information must also "derive independent economic value . . . from not being generally known." *Id.* "To establish the misappropriation element, [the] plaintiff must show"—

> (A) acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or
>
> (B) disclosure or use of a trade secret of another without express or implied consent by a person who—
>
>> (i) used improper means to acquire knowledge of the trade secret;
>>
>> (ii) at the time of disclosure or use, knew or had reason to know that the knowledge of the trade secret was—
>>
>>> (I) derived from or through a person who had used improper means to acquire the trade secret;
>>>
>>> (II) acquired under circumstances giving rise to a duty to maintain the secrecy of the trade secret or limit the use of the trade secret; or
>>>
>>> (III) derived from or through a person who had owed a duty to the person seeking relief to maintain the secrecy of the trade secret or limit the use of the trade secret . . .

Tang v. E. Va. Med. Sch., No. 2:20cv575, 2021 WL 2916714, at *6–7 (E.D. Va. July 12, 2021) (quoting 18 U.S.C. § 1839(5)).

"A plaintiff must identify, with particularity, each trade secret it claims was misappropriated." *MicroStrategy*, 331 F. Supp. 2d at 418. The Court, in turn, must determine if each individual trade secrets satisfies each element. *Id.* at 420. ("[T]he court must assess each alleged trade secret according to the requisite elements.").

2. Synopsys's Motion for Summary Judgment

Synopsys outlines myriad grounds in support of its motion for summary judgment on this Count. Some of Synopsys's arguments apply to only subsets of RBS's asserted trade secrets: RBS did "[n]ot [s]ufficiently [i]dentif[y]" one group of trade secrets; Black Duck "[n]ever [h]ad [a]ccess to" another; and Black Duck "[h]ad a [l]icense to [a]ccess, [u]se and [s]hare" another. (ECF No. 227, at 19, 32.) The Court finds that many of these shortcomings could be fatal to RBS's claims for those particular trade secrets.[43] But other alleged shortcomings apply to all of RBS's claimed trade secrets, and two of them warrant summary judgment in its entirety on this Count.[44] *Celotex,*

---

[43] For example, the Court could grant summary judgment in Synopsys's favor for Trade Secrets 5–6 and 19–23 because, in those trade secrets, RBS cites material in documents Black Duck created. RBS finds this appropriate because the Black Duck documents contain "information *extracted from VulnDB.*" (ECF No. 341, at 23 (emphasis in original).) But, fatal to its claim, RBS has not shown that the Black Duck materials constituted mere copies or reproductions of RBS's preexisting lists or compilations and, in fact, did not identify where in its own products this material originated. *Cf. Ozburn-Hessey Logistics, LLC v. 721 Logistics, LLC*, 13 F. Supp. 3d 465, 475 (E.D. Pa. 2014) (finding that the plaintiff could not "claim trade-secret protection for a customer list produced by someone else," but noting that "the situation would [have] be[en] different" if the customer list "was merely a reproduction of a list that already existed at" the plaintiff's company).

[44] The Court will deny the portions of Synopsys's motion on any grounds for which the parties dispute material facts. For example, Synopsys argues that none of RBS's claimed trade secrets qualify for protection because they are publicly known and readily ascertainable. But the public availability of material does not necessarily render that material "readily ascertainable by proper means." *Hoechst Diafoil Co. v. Nan Ya Plastics Corp.*, 174 F.3d 411, 419 (4th Cir. 1999); *see AirFacts, Inc. v. de Amezaga*, 909 F.3d 84, 96 (4th Cir. 2018) (concluding that a product "contain[ed] information not readily ascertainable to outsiders . . . [t]hough anyone with a subscription c[ould] access the [underlying] data"); *Compulife Software Inc. v. Newman*, 959 F.3d 1288, 1314 (11th Cir. 2020) ("Nor does the fact that the defendants took the quotes from a publicly accessible site automatically mean that the taking was authorized or otherwise proper."). Because the parties

477 U.S. at 322 ("[T]he plain language of Rule 56(c) mandates the entry of summary judgment, after adequate time for discovery and upon motion, against a party who fails to make a showing sufficient to establish the existence of an element essential to that party's case, and on which that party will bear the burden of proof at trial."). The Court addresses both in turn.

A. *Independent Economic Value*

To establish that material constitutes a trade secret, a plaintiff must show that the trade secret "[d]erives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use." Va. Code § 59.1-336; *see also* 18 U.S.C. § 1839(3) (the material must "derive independent economic value . . . from not being generally known"). The Court must determine whether "*each* alleged trade secret" satisfies this element. *See MicroStrategy*, 331 F. Supp. 2d at 420 (emphasis added).

Here, RBS reasons that its trade secrets have independent economic value because "RBS was acquired in January for $85 million," and "[a]t least 90% of RBS's revenues come from Vul-nDB." (ECF No. 341, at 28.) This illative argument fails for two reasons. First, RBS has not established a connection between the January 6 acquisition, RBS's revenues, VulnDB, and any particular trade secret. Because the Court must determine whether each trade secret satisfies this requisite element, RBS's failure to link any asserted trade secret to the company's value proves fatal.[45]

---

dispute facts regarding the availability of the material RBS claims as trade secrets, the Court will reserve ruling on this fact-intensive issue until trial.

[45] In *Trandes Corp. v. Guy F. Atkinson Co.*, the plaintiff claimed as a trade secret its object code. 996 F.2d 655, 663 (4th Cir. 1993). The court found that, "[a]rmed with a copy of the object code, an individual would have the means to offer much the same . . . services as" the plaintiff. *Id.*

Even if that were not the case, the timing of this evidence renders it irrelevant. Flashpoint Intel ("Flashpoint") acquired RBS on January 6, 2022. (ECF No. 181.) At that time, RBS had identified approximately 150 trade secrets that it asserted Synopsys misappropriated. (ECF No. 188-7, at 25–47.) After the Flashpoint acquisition, RBS revised, replaced, and added to this list, resulting in 160 alleged trade secrets.[46] (ECF No. 188-8, at 49–76.) Weeks later, RBS narrowed its focus, stating that it would assert that Synopsys misappropriated only about half of these trade secrets. The Court has no method—and RBS has likewise suggested none—of determining which of the now-asserted trade secrets, if any, contributed to RBS's valuation on January 6, 2022. Because RBS has failed to establish which, if any, of its trade secrets possess independent economic value, the Court will grant summary judgment on this Count.[47]

Because the plaintiff's services "generate[d] substantial revenues," the Court concluded that the object code also carried independent economic value. *Id.*

Like the plaintiff in *Trandes*, RBS receives most of its revenues from a singular service. Unlike the plaintiff in *Trandes*, though, RBS has not claimed that an individual could replicate this service by using just one of RBS's asserted trade secrets. Absent this connection, RBS's VulnDB revenues do not prove independent economic value for any particular trade secret.

[46] RBS's (now-excluded) expert, Kursh, cites these 160 trade secrets in his report. (*See* ECF No. 187, at 8.)

[47] RBS also argues that "there is, in fact, a market for portions of VulnDB." (ECF No. 341, at 29.) In support, RBS cites its cofounder's statement that some clients are "only interested in certain elements that reside within VulnDB." (ECF No. 341-6, at 13:8–15.) RBS's cofounder clarifies, though, that these clients do not seek elements of or access to RBS's database. Rather, they seek "to be alerted if a certain product was found to be vulnerable." (*Id.* at 14:11–22.) Because RBS has not shown that it claimed a trade secret in such alerts or how the Court could calculate the economic value of such a trade secret, this evidence proves irrelevant as to economic value.

B. *Reasonable Efforts to Maintain Secrecy*

Even if RBS had sufficiently established that any or all of RBS's trade secrets possess independent economic value, RBS has not shown that it took reasonable efforts to maintain the secrecy of its asserted trade secrets.

Whether a party "took reasonable efforts to maintain the secrecy of its purported trade secrets is a 'fact intensive' question." *Young Design, Inc. v. Teletronics Int'l, Inc.*, No. CIV.A. 00-970-A, 2001 WL 35804500, at *6 (E.D. Va. July 31, 2001) (quoting *Hoechst*, 174 F.3d at 418). "[R]easonable efforts to maintain secrecy need not be overly extravagant, and absolute secrecy is not required." *Chmura Econ. & Analytics, LLC v. Lombardo*, No. 3:19cv813, 2021 WL 3234607, at *16 (E.D. Va. July 29, 2021) (quoting *AvidAir Helicopter Supply, Inc. v. Rolls-Royce Corp.*, 663 F. 3d 966, 974 (8th Cir. 2011)).

> Simply because information is disclosed outside of a company does not result in the loss of trade secret status. "'The secrecy need not be absolute; the owner of a trade secret may, without losing protection, disclose it to a licensee, an employee, or a stranger, if the disclosure is made in confidence, express or implied.'" *Tao of Sys. Integration, Inc. v. Analytical Servs. & Materials, Inc.*, 299 F. Supp. 2d 565, 574 (E.D. Va. 2004) (quoting *Dionne v. Southeast Foam Converting & Packaging, Inc.*, 240 Va. 297, 397 S.E.2d 110, 113 (1990)). Furthermore, the requirement that the information not be generally known refers to the knowledge of other members of the relevant industry—the persons who can gain economic benefit from the secret. *See* Uniform Trade Secrets Act, § 1, comment. Finally, only reasonable efforts must be taken to maintain secrecy. Restricting access to information, implementing confidentiality agreements, and providing physical barriers to access are all reasonable efforts.

MicroStrategy, 331 F. Supp. 2d at 416.

In general, RBS tells potential customers about its confidentiality requirements and requires that they sign a "nondisclosure agreement." (ECF No. 341-6, at 15:15–22; *see also* ECF

29

No. 341-10.)[48] But the evidence also shows that, in some of its licensing agreements, RBS failed to take reasonable efforts to protect its trade secrets. For example, in 2012 RBS entered into an agreement with IBM that allowed IBM to, among other rights, not only "access . . . VulnDB," but also to "copy, modify, adapt, and incorporate . . . VulnDB into" its products; "to prepare and have prepared derivative works of VulnDB so accessed and incorporated"; and "to grant others the rights granted herein." (ECF No. 234-13, at 3.) In other words, the agreement allowed IBM to incorporate VulnDB into its own products and then sell access to VulnDB, through those products, to its customers. Though the RBS-IBM agreement contained certain restrictions on the license of VulnDB to end users, those end user restrictions did not include confidentiality requirements. And even if the RBS-IBM agreement is, as RBS claims, an "outlier," the Court finds significant that RBS failed to protect the confidentiality of the information for which it now claims trade secret protection in an agreement with IBM—a global company that, in 2012, boasted $104.5 billion in revenue and served thousands of clients.[49]

RBS similarly failed to protect the secrecy of its claimed trade secrets in the Reseller Agreement by not requiring Black Duck to obtain confidentiality agreements from its customers.[50] Perhaps in a different context this fact would not weigh so heavily into the Court's analysis. But

---

[48] RBS brought "hundreds of [nondisclosure agreements]" to the March 1, 2022 hearing on this motion. (ECF No. 396, at 89:21–22.)

[49] *See, e.g.*, IBM, *2012 IBM Annual Report* 1, 13, https://www.ibm.com/investor/att/pdf/IBM_Annual_Report_2012.pdf (last accessed Mar. 23, 2022).

[50] The agreement also permitted Black Duck—in its sole discretion—to assign the agreement, or any of its rights under the agreement, without RBS's consent. (ECF No. 221-11 § 13.8.) Because any assignee would remain subject to the confidentiality provisions that then applied to Black Duck, the Court does not find this assignment provision dispositive. (*Id.*); *see O'Malley v. Moghul*, 55 Mass. App. Ct. 1113, 773 N.E.2d 478, 2002 WL 1931998, at *1 (2002) (Table) ("The general assignment of a contract . . . includes both an assignment of rights and a delegation of contract duties, unless the circumstances surrounding the assignment show a contrary intent.").

30

here, the agreement's very purpose was for Black Duck "to incorporate [VulnDB] into [its] products." (ECF No. 221-11, at 2.) Black Duck could do so by "us[ing], reproduc[ing] and hav[ing] reproduced, and embed[ding] or hav[ing] embedded" VulnDB into its products, and then "distribut[ing], sell[ing] and offer[ing] to sell access to" VulnDB to end users through those products. (*Id.* §§ 2.2.1, 2.2.2.) RBS understood and intended for Black Duck to resell the product to customers, but nevertheless did not require that Black Duck include confidentiality provisions in its end user agreements. As a result, RBS retained no control over whether Black Duck's agreements with its end users expressly or implicitly also required confidentiality. Although "[the] necessary element of secrecy is not lost . . . if the holder of the trade secret reveals the trade secret to another 'in confidence, and under an implied obligation not to use or disclose it,'" the evidence here shows that RBS consistently failed to take reasonable steps to keep secret the material it now seeks to protect. *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 475 (1974) (quoting *Cincinnati Bell Foundry Co. v. Dodds*, 10 Ohio Dec. Reprint 154, 156 (Super. Ct. 1887)). The Court will also grant Synopsys's motion for summary judgment on this Count for this reason.

3. RBS's Motion for Summary Judgment

A. *Use or Acquisition of Trade Secrets 1–5, 7–11, 19, and 68*

RBS seeks summary judgment for the use or acquisition elements of trade secret misappropriation for Trade Secrets 1–5, 7–11, 19, and 68. The Court has already granted Synopsys's motion for summary judgment for a declaratory judgment of no trade secret misappropriation as to all of RBS's asserted trade secrets. Even if it had not yet done so, though, the Court would deny this portion of RBS's motion.

Both the DTSA and the VUTSA define "misappropriation" as "acquisition of a *trade secret*" or "disclosure or use of a *trade secret*." 18 U.S.C. § 1839(5) (emphasis added); Va. Code

§ 59.1-336 (emphasis added).[51] Whether an item satisfies the elements of a trade secret thus con-stitutes a necessary prerequisite for misappropriation. *See Graystone Funding Co., LLC v. Network Funding, L.P.*, No. 2:19cv383, 2021 WL 4460113, at *3 (D. Utah Sept. 29, 2021) ("To es-tablish a claim for misappropriation of trade secrets under . . . the DTSA, . . . the proponent of the trade secret must first demonstrate the existence of a trade secret."). Because RBS has not shown that any of its material satisfies the requirements for a trade secret,[52] the Court will deny RBS's partial motion for summary judgment on these elements.

B. *Independent Development Defense*[53]

RBS seeks summary judgment on the independent development defense because Synop-sys has "fail[ed] to back up" its assertions about its cybersecurity research and independent access, research, and development "with corroborating evidence." (ECF No. 228, at 32.) Though inde-pendent development serves as a valid defense to a claim of trade secret misappropriation,[54] there are genuine and material factual disputes regarding Black Duck's efforts to independently develop its products. (*See* ECF No. 228, at 32–33; ECF No. 328, at 22–24.) Had the Court not granted

---

[51] The statutes, in turn, define a "trade secret" as an item that satisfies specific requirements. 18 U.S.C. § 1839(3); Va. Code § 59.1-336.

[52] *See supra* Section B.b.2.

[53] As it did with the unclean hands defense, Synopsys denies asserting this affirmative defense but nevertheless argues that it remains "entitled" to introduce related evidence. (ECF No. 328, at 23 n.5.) For the reasons outlined in note 39, the Court finds it proper to consider the defense at this time. (*See also* ECF No. 1 ¶ 60 (Synopsys's complaint) (stating in support of Count II that Synopsys "used independent research and development, public knowledge and [its] own innova-tions to create Synopsys' business, technology and products.").)

[54] *Kewanee*, 416 U.S. at 476 (noting that trade secret laws "do[] not offer protection against discovery by fair and honest means, such as by independent invention").

summary judgment on Count II, it would have denied this portion of RBS's motion for summary judgment and weighed the relevant evidence at trial.

c. Count IV: Declaratory Judgment of No Tortious Interference

Synopsys says that the Court should grant summary judgment on this claim because RBS "has not identified any facts that would support a *prima facie* claim of tortious interference, including the existence of any particular business expectancy, Synopsys' knowledge of the expectancy, or any harm to RBS' expectancy." (ECF No. 227, at 36.)

To prove tortious interference under Virginia law, the plaintiff must show:

(1) the existence of a valid contractual relationship or business expectancy;
(2) knowledge of the relationship or expectancy on the part of the interferor;
(3) intentional interference inducing or causing a breach or termination of the relationship or expectancy; and
(4) resultant damage to the party whose relationship or expectancy has been disrupted.

Creech v. Everbank, 467 F. Supp. 3d 425, 434 (E.D. Va. 2020) (quoting *Masco Contractor Servs. E., Inc. v. Beals*, 279 F. Supp. 2d 699, 709 (E.D. Va. 2003)). "The evidence of an expectancy must establish expectancy by and between two parties at least, based upon something that is a concrete move in that direction." *GEICO v. Google, Inc.*, 330 F. Supp. 2d 700, 705 (E.D. Va. 2004) (dismissing claim where the plaintiff failed "to plead a specific, existing contract or expectancy with a specific party" (quoting *Moore v. United Int'l Investigative Servs., Inc.*, 209 F. Supp. 2d 611, 619–20 (E.D. Va. 2002)).

RBS broadly asserts that Synopsys interfered with "its business expectancies" and, in support, cites an email in which a Synopsys employee states that the company should "be prepared to more aggressively migrate customers over to BDSA if [RBS] take[s] more aggressive actions." (ECF No. 341-12, at 20.) RBS argues that "[e]ach time Synopsys migrated a customer from VulnDB to BDSA, it interfered with RBS's expectancy of vulnerability intelligence business with that

33

customer." (ECF No. 341, at 35.) This vague statement reflects the harsh reality of a competitive market, but lacks the specificity required to prevail on a tortious interference claim. Because RBS has not presented evidence of any "specific, existing contract or expectancy with a specific party," the Court will grant Synopsys's motion for summary judgment on this Count. *GEICO*, 330 F. Supp. 2d at 705–06.

III. CONCLUSION

For the reasons explained above, the Court will grant in part and deny in part each party's motion to exclude, (ECF Nos. 206, 233), grant Synopsys's motion for summary judgment as to Counts II and IV and deny its motion as to Count I, (ECF No. 218), and grant RBS's motion for partial summary judgment as to Synopsys's unclean hands defense but deny RBS's motion for partial summary judgment in all other respects, (ECF No. 219). The Court issued an Order with these rulings on March 2, 2022, (ECF No. 394), and will issue a separate Order that sets out its judgment as to Counts II and IV under Rule 58.

Let the Clerk send a copy of this Opinion to all counsel of record and to the Special Master.

Date: 28 July 2022
Richmond, VA

/s/
John A. Gibney, Jr.
Senior United States District Judge